Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi

Statsrådets principbeslut om en nationell informationssäkerhetsstrategi

Government Resolution on National Information Security Strategy

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Helsinki, 2009

LIIKENNE- JA VIESTINTÄMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä
4.12.2008

Tekijä	Julkaisun laji
Arjen tietoyhteiskunnan neuvottelukunnan alainen	Periaatepäätös
tietoturvallisuusryhmä, pj. Juhapekka Ristola, siht.	Toimeksiantaja Liikenne- ja viestintäministeriö
Mari Herranen	Toimielimen asettamispäivämäärä

Julkaisun nimi

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi

Tiivistelmä

Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta ”Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –” hyväksyttiin valtioneuvoston istunnossa 4.12.2008. Strategian tavoitteena on luoda suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Yleisen tietoturvaosaamisen pitää olla korkealla tasolla, ja yhteiskunnan eri tahot toimivat saumattomassa yhteistyössä tietoturvan edistämiseksi. Suomi on tietoturvan edelläkävijämaa maailmassa vuonna 2015. Strategiassa on kolme painopistettä: 1) Perustaidot arjen tietoyhteiskunnassa, 2) Tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä 3) Kilpailukyky ja kansainvälinen verkostoyhteistyö.

Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta, se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Liikenne- ja viestintäministeriön asettama Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä tukee tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Tavoitteiden saavuttamiseksi periaatepäätöksen painopisteiden pohjalta tehdään toimenpideohjelma. Strategian toteutuksen kannalta tarpeelliset toimenpiteet, mittarit ja seuranta sisältyvät toimenpideohjelmaan, joka valmistuu keväällä 2009.

Edellinen valtioneuvoston periaatepäätös kansalliseksi tietoturvallisuusstrategiaksi hyväksyttiin vuonna 2003. Tietoturvallisuusstrategia nosti tietoturvan merkittäväksi toimijaksi yhteiskunnalliseen keskusteluun, ja tietoturvatietämys ja -ymmärrys ovat kasvaneet. Uusi tietoturvastrategia laadittiin vuoden 2008 aikana arjen tietoyhteiskunnan neuvottelukunnan alaisessa tietoturvallisuusryhmässä. Arjen tietoturvallisuusryhmän tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi.

Avainsanat (asiasanat)

tietoturva

Muut tiedot

Yhteyshenkilö/LVM Mari Herranen

Sarjan nimi ja numero	ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisuja 62/2008	1457-7488 (painotuote) 1795-4045 (verkkojulkaisu)	978-952-243-004-5 (painotuote) 978-952-243-005-2 (verkkojulkaisu)
Sivumäärä (painotuote)	Kieli	Luottamuksellisuus
52	suomi/ruotsi/englanti	julkinen
Jakaja	Kustantaja	
Liikenne- ja viestintäministeriö	Liikenne- ja viestintäministeriö	

KOMMUNIKATIONSMINISTERIET

PRESENTATIONSBLAD

Utgivningsdatum
4.12.2008

Författare	Typ av publikation
Gruppen för informationssäkerheten i vardagens informationssamhälle, Juhapekka Ristola (ordf.), Mari Herranen (sekr.)	Principbeslut
	Uppdragsgivare: Kommunikationsministeriet
	Datum för tillsättandet av organet

Publikation

Statsrådets principbeslut om en nationell informationssäkerhetsstrategi ”Trygg vardag i informationssamhället – Inte med tur utan med kunskap"

Referat

Statsrådets principbeslut om en nationell informationssäkerhetsstrategi ”Trygg vardag i informationssamhället – Inte med tur utan med kunskap" godkändes av statsrådet 4.12.2008. Med hjälp av den nationella informationssäkerhetsstrategin strävas det efter att skapa finländarna (medborgare, företag, myndigheter och andra aktörer) en trygg vardag i informationssamhället. Strategin har den visionen att medborgarna och företagen kan lita på att deras uppgifter är säkra både på data- och kommunikationsnäten och i tjänsterna som hör till dem. Det allmänna informationssäkerhetskunnandet ska vara på en hög nivå och olika parter i samhället samarbetar friktionsfritt i syfte att främja informationssäkerheten. Finland är föregångarlandet i informationssäkerheten i världen 2015. Strategin har tre tyngdpunkter: 1) Baskunskaper i vardagens informationssamhälle, 2) Riskhantering som anknyter till information och funktionssäkerhet, och 3) Konkurrenskraft och internationellt nätverkssamarbete.

Statsrådet bär helhetsansvaret för informationssäkerhetsstrategin och övervakar genomförandet av strategin och uppdaterar den efter behov. Gruppen för informationssäkerheten i vardagens informationssamhälle som tillsatts av kommunikationsministeriet stöder samordningen av åtgärderna som genomförandet av strategin kräver samt följer hur strategin verkställs. För att målen kan nås utarbetas det utifrån tyngdpunkterna i principbeslutet ett åtgärdsprogram. Åtgärderna, mätarna och uppföljningen som är nödvändiga med tanke på genomförandet av strategin ingår i åtgärdsprogrammet som blir färdigt våren 2009.

Statsrådets föregående principbeslut om en nationell strategi för informationssäkerheten antogs 2003. Strategin lyfte fram informationssäkerheten till ett betydande tema i den samhälleliga debatten och syn på och förstånd om informationssäkerheten har vuxit. En ny strategi skapades under 2008 i informationssäkerhetsgruppen som lyder under delegationen för vardagens informationssamhälle. Gruppen för informationssäkerheten i vardagens informationssamhälle har till uppgift att främja informationssäkerheten i informationssamhället, följa utvecklingen i fråga om informationssäkerhet och att ta initiativ till att förbättra informationssäkerheten.

Nyckelord

informationssäkerhet

Övriga uppgifter

Kontaktperson vid ministeriet är Mari Herranen.

Seriens namn och nummer	ISSN	ISBN
Kommunikationsministeriets publikationer 62/2008	1457-7488 (trycksak) 1795-4045 (nätpublikation)	978-952-243-004-5 (trycksak) 978-952-243-005-2 (nätpublikation)
Sidoantal (trycksak): 52	Språk: finska/svenska/engelska	Sekretessgrad: offentlig
Distribution: Kommunikationsministeriet	Förlag: Kommunikationsministeriet	

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

DESCRIPTION

Date of publication
4.12.2008

Author	Type of publication
Information Security Group of the Ubiquitous	Government Resolution
Information Society Advisory Board, Juhapekka	Assigned by Ministry of Transport and Communications
Ristola (chair), Mari Herranen (secretary)	Date when body appointed

Name of the publication

Government Resolution on National Information Security Strategy

Abstract

The Government Resolution on National Information Security Strategy "Everyday security in the information society - a matter of skills, not of luck." was adopted by the Finnish Government on the 4th of December 2008. The aim of the National Information Security Strategy aims to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and for businesses, administrative authorities, and all other actors in society. The Strategy's vision is that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services. There must be a high overall level of information security skills and knowhow, and the different actors in society need to work seamlessly together to improve information security. By 2015 Finland will be the leading country in the world in terms of information security. There are three priority areas in the Strategy; 1) Basic skills in the ubiquitous information society, 2) Information risk management and process reliability, and 3) Competitiveness and international network cooperation.

The overall responsibility for the National Information Security Strategy lies with the Government, which supervises the Strategy's implementation and updates it when necessary. The Information Security Group of the Ubiquitous Information Society Advisory Board appointed by the Ministry of Transport and Communications supports the coordination of the Strategy's implementation and monitors the implementation process. In order to attain the Strategy's goals, an action plan will be drawn up based on the priorities set out in this Resolution. The measures, indicators, monitoring and follow-up necessary for the implementation of the Strategy will be included in the action plan, which will be completed by spring 2009.

The previous government resolution on national information security strategy was adopted in 2003. The strategy drew attention to and encouraged discussion about information security and awareness. The Strategy of 2008 was drawn up by the Information Security Group that works under the Ubiquitous Information Society Advisory Board. The tasks of the Information Security Group are to promote information security in the information society, monitor the progress that is made, and suggest improvements.

Keywords

information security

Miscellaneous

Contact person at the Ministry: Ms Mari Herranen

Serial name and number	ISSN	ISBN
Publications of the Ministry of Transport and Communications 62/2008	1457-7488 (printed version) 1795-4045 (electronic version)	978-952-243-004-5 (printed version) 978-952-243-005-2 (electronic version)
Pages, total (printed version)	Language	Confidence status
52	Finnish/Swedish/English	Public

Distributed and published by

Ministry of Transport and Communications

Sisällys/Innehåll/Content

Liitteet / Bilagorna / Appendices

VALTIONEUVOSTON PERIAATEPÄÄTÖS KANSALLISESTA TIETOTURVASTRATEGIASTA
"Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –"

Strategian tavoitteet

Kansallisen tietoturvastrategian avulla pyritään luomaan suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Yleinen tietoturvaosaamisen pitää olla korkealla tasolla ja yhteiskunnan eri tahot toimivat saumattomassa yhteistyössä tietoturvan edistämiseksi. Suomi on tietoturvan edelläkävijämaa maailmassa vuonna 2015.

Painopiste 1: Perustaidot arjen tietoyhteiskunnassa

Painopiste 2. Tietoihin liittyvien riskien hallinta ja toimintavarmuus

Painopiste 3: Kilpailukyky ja kansainvälinen verkostoyhteistyö

Toimenpiteet

Painopiste 1: Perustaidot arjen tietoyhteiskunnassa

Jokainen tietoyhteiskunnan toimija vaikuttaa teoillaan sekä omaan että muiden tietoturvallisuuteen. Siksi on tärkeää, että kaikilla on tietoturvallisuudesta riittävät perustiedot ja -taidot. Luottamus tietoyhteiskuntaa kohtaan syntyy, kun sekä palveluiden käyttäjät että tuottajat ymmärtävät vastuunsa, oikeutensa ja velvollisuutensa.

Palveluiden käyttäjien tulee kyetä tunnistamaan ja tiedostamaan turvallisen ja luotettavan palvelun lähtökohdat. Sähköisen asioinnin kansalaistaidot ja verkkolukutaito ovat edellytyksiä turvalliselle liikkumiselle verkossa. Riskien ennakointi, tunnistaminen ja niihin varautuminen säästää monelta ikävältä yllätykseltä. Erityisesti **palvelun tarjoajan** tulee varmistaa palveluiden käytön turvallisuus sekä osaltaan huolehtia luottamuksellisten tietojen tunnistamisesta ja suojaamisesta. Palvelun tarjoajalla on myös velvollisuus huolehtia palvelun turvallisuuden jatkuvasta ylläpitämisestä palvelu- ja toimintaympäristön muuttuessa.

Avoin ja selkeä viestintä palvelun turvallisuudesta ja mahdollisista riskeistä luo perustan sille luottamukselle, jota arjen tietoyhteiskunnassa toimimisessa tarvitaan. Palvelun tarjoajan vastuuta ei voi ulkoistaa. Käytännössä palvelun tarjoaja vastaa palvelun tuottamiseen osallistuvien toimijoiden kanssa palvelun tietoturvallisuudesta.

Strategian tehtävänä on integroida tietoturva kiinteäksi osaksi tietoyhteiskunnan perusrakenteita. Tämä edellyttää paitsi yleisen tietoturvatietoisuuden ja -osaamisen vahvistamista myös tietoturvanäkökohtien huomioon ottamista järjestelmähankinnoissa ja sopimusprosesseissa.

- **Tietoturvatietoisuuden ja -osaamisen vahvistaminen**

    - Kehitetään kansallista tietoturvapäivä-hanketta
    - Lisätään tietoturvatietoisuutta, seurataan tietoisuuden tasoa ja kehitetään tietoturvaosaamista
    - Laaditaan aktiivinen ja ennakoiva viestintäsuunnitelma

- **Turvallisten sähköisten palveluiden tarjoaminen ja luottamuksellisuuden varmistaminen**

    - Lisätään tietoturvavaatimukset osaksi jokaista tarjouspyyntöä, ml. ratkaisujen ja palvelujen suunnitteluvaiheet
    - Edistetään tietoturvaratkaisujen laajempaa käyttöä
    - Selvitetään mahdollisuutta kehittää turvallisille palveluille myönnettävää erillistä sertifikaattia
    - Edistetään sertifioitujen tietoturva-ammattilaisten määrän lisäämistä Suomessa

Painopiste 2. Tietoihin liittyvien riskien hallinta ja toimintavarmuus

Sähköiset palvelut ja asiointi muodostavat yhä keskeisemmän osan niin julkisen kuin yksityisen sektorin palvelujärjestelmää. Samalla riippuvuus tietotekniikasta tekee palveluista entistä haavoittuvaisempia. Erilaisia viestintäpalveluita käyttävien kansalaisten on voitava luottaa, että palveluiden käyttö on turvallista ja että luottamuksellisia tietoja ei joudu vääriin käsiin. Kansalaisille ja yrityksille tulee taata riittävä viranomaistuki, jos tietoturvaa on loukattu esimerkiksi identiteettivarkaus-tapauksissa.

Kun ulkoistetaan palveluita ja ketjutetaan hankintoja, on varmistettava tietoturvan kokonaisvaltainen hallinta. Palveluita suunniteltaessa tulee koko verkon tietojen turvallisuus arvioida kokonaisvaltaisesti. Tässä palvelun tarjoajalla on keskeinen vastuu. Tietojen luottamuksellisuus, tietojen eheys ja käytettävyys ovat oleellisia asioita palvelussa.

Tietoyhteiskunnan kriittisen infrastruktuurin toimivuus ja tieto- ja viestintäjärjestelmien sekä viestintäpalveluiden turvallisuus tulee varmistaa kaikissa tilanteissa -normaalioloista poikkeusoloihin asti. Yritysten toiminnan jatkuvuus ja kansalaisten palveluiden saatavuus on varmistettava.

- **Riskienhallinnan ja toimintavarmuuden kehittäminen**

    - Tuetaan yritysten käyttöön tarkoitettujen riskienhallintamallien laajempaa käyttöönottoa
    - Järjestetään riskienhallintaan liittyvää koulutusta

- **Yhteiskunnan elintärkeiden toimintojen turvaaminen kaikissa tilanteissa**

    - Selvitettävä mitä menetelmiä ja varautumismalleja tulee kehittää entistä monimutkaisempien verkkojen ja verkostojen hallintaan
    - Selvitetään mahdollisuutta tukea yritysten varautumis- ja riskienhallintatoimintaa
    - Tuetaan lainsäädännöllisin keinoin yhteiskunnan elintärkeiden toimintojen tarvitsemien viestintäverkkojen ja viestintäpalvelujen toiminnan varmistamista

Painopiste 3: Kilpailukyky ja kansainvälinen verkostoyhteistyö

Suomen tulee kehittää omaa kansallista sääntely-ympäristöään yritysten kannalta yksinkertaisempaan ja ennustettavampaan suuntaan sekä pyrkiä aktiivisesti vaikuttamaan kansainväliseen sääntelyyn. Kansallisen lainsäädännön selkeys ja liiketoiminnan esteiden poistaminen vaikuttavat olennaisesti kansalliseen kilpailukykyyn ja yritysten haluun investoida Suomeen. Lisäksi on huolehdittava siitä, että erot tietoturvaan liittyvien EU-direktiivien kansallisessa toimeenpanossa eivät kohtuuttomasti vaikeuta useassa EU-maassa toimivien suomalaisten yritysten toimintaa. Kilpailukykyisen tietoyhteiskunnan kannalta on välttämätöntä, että sen keskeinen tietopääoma kuten teollisoikeudet ja yrityssalaisuudet on suojattu. Näillä toimenpiteillä voidaan turvata yritysten toiminta Suomessa ja suomalaisten yritysten toiminta ulkomailla sekä lisätä Suomen houkuttelevuutta yritysten sijoittautumisessa.

Suomi on osa globaalia tietoverkkotaloutta ja suurin osa tietoturvauhista ja -hyökkäyksistä kohdistuu meihin maamme rajojen ulkopuolelta. Näiden uhkien torjuminen edellyttää paitsi kattavaa varautumista ja toimivia kansainvälisiä yhteistyöverkostoja myös ennakoivaa toimintaotetta ja heikkojen signaalien tunnistamista. Suomen tulee toimia aktiivisesti kansainvälisessä viranomaisyhteistyössä tietoturvauhkien ennaltaehkäisemiseksi ja haittojen vähentämiseksi. Globalisaatio ei ole ainoastaan uhka, vaan myös mahdollisuus. Toimiakseen vaikuttavasti kansainvälisillä foorumeilla Suomen tulee kyetä priorisoimaan kansainvälistä toimintaansa ja kohdistamaan resurssinsa tietoturvan kannalta keskeisiin kysymyksiin. Vaikuttavaan toimintaan päästään ainoastaan hyvällä kansallisella yhteistyöllä ja etukäteisvaikuttamisen kautta.

- **Suomen houkuttelevuuden ja kilpailukyvyn vahvistaminen ennustettavuutta lisäämällä**

    - Kansainvälisten standardien käyttöönoton edistäminen sekä aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön
    - Vaikutetaan EU-yhteistyön kautta siihen, että tietoturvaan liittyvät direktiivit toimeenpannaan mahdollisimman yhdenmukaisesti, joka edistää useassa maassa toimivien suomalaisten yritysten toimintaa

- **Ennakoivan ja vaikuttavan kansainvälisen yhteistyön terävöittäminen**
    - Harkitaan kansallisen kv-yhteistyöverkoston perustamista, jossa tieto ja kokemukset kv-työryhmistä leviävät
    - Selvitetään Suomen kansallisen tietoliikenneturvallisuusviranomaisen (NCSA) perustamisen tarvetta

Strategian toimeenpano

Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Liikenne- ja viestintäministeriön asettama arjen tietoyhteiskunnan tietoturvallisuus -ryhmä tukee tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategia sekä raportoi arjen tietoyhteiskunnan neuvottelukunnalle työn etenemisestä.

Tavoitteiden saavuttamiseksi periaatepäätöksen painopisteiden pohjalta tehdään toimenpideohjelma. Strategian toteutuksen kannalta tarpeelliset toimenpiteet, mittarit, ja seuranta sisältyvät toimenpideohjelmaan, joka valmistuu keväällä 2009.

VALTIONEUVOSTON PERIAATEPÄÄTÖKSEN PERUSTELUMUISTIO KANSALLISESTA TIETOTURVASTRATEGIASTA

”Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –”

Strategian tausta

Kansallisessa tietoyhteiskuntakehityksessä eletään vaihetta, jossa aikaisemmin erillisenä toimintalohkona ollut tieto- ja viestintäteknologia on muuttunut osaksi kansalaisten jokapäiväistä arkea. Arjen tietoyhteiskunnassa (ns. ubiikkiyhteiskunta) tietotekniset ratkaisut monipuolistuvat ja muuttuvat käyttäjien kannalta kiinteäksi osaksi ihmisten ja yritysten normaalitoimintaa. Tämän takia on oleellista, että kansalaiset voivat käyttää tietoyhteiskunnan palveluita vaivatta ja että sähköiset palvelut koetaan luotettaviksi. Tämä on kaikkien vastuulla ja siksi tietoturvaosaaminen ja -tiedostaminen ovat oleellisen tärkeitä asioita. Tavoitteena on turvallinen arki tietoyhteiskunnassa, ei tuurilla vaan taidolla. Tietojen luottamuksellisuuden, eheyden ja käytettävyyden merkitys on suuri tämän päivän arjen tietoyhteiskunnassa.

Edellinen valtioneuvoston periaatepäätös kansalliseksi tietoturvallisuusstrategiaksi hyväksyttiin vuonna 2003 ja se kokosi lähes ainutlaatuisella tavalla sekä yksityisen että julkisen sektorin toimijat saman pöydän ääreen. Ennen kaikkea strategia nosti tietoturvan merkittäväksi aiheeksi yhteiskunnalliseen keskusteluun. Tietoturvatietämyksemme ja ymmärryksemme on kasvanut ja Suomi on voinut edustaa eturivin maita tietoturva-asioissa sekä EU:ssa että kansainvälisillä foorumeilla. Tietoturvallisuusstrategia oli ensimmäinen Euroopassa ja mahdollisesti ensimmäinen maailmassa. Tietoturvallisuusstrategian ja sen toteutusta koordinoivan kansallisen tietoturvallisuusasioiden neuvottelukunnan toimikausi loppui keväällä 2007. Tätä työtä tehtiin hyvin vahvasti julkisen ja yksityisen sektorin välisenä yhteistyönä. Tietoturvallisuusstrategian suurimmat tulokset olivat tietoturvatietoisuuden lisääntyminen, mm. kansallisen tietoturvapäivän luomisella, kansallisen tietoturvatilannekuvan muodostaminen sekä ”Luottamus ja tietoturva sähköisissä palveluissa” -kehittämisohjelman puitteissa saavutetut tulokset.

Toimintaympäristö muuttuu nopeasti ja sen takia on tarve päivittää tietoturvastrategia. Tärkeää on saada realistinen ja fokusoitu kansallinen tietoturvastrategia, jossa on muutamia priorisoituja tavoitteita. Tietoturvasta on tehtävä olennainen ja luonteva osa jokapäiväistä elämää. Strategiaa ei tämän takia kirjoiteta vain alan asiantuntijoille. Strategialla ei vain passiivisesti reagoida vaan vaikutetaan aktiivisesti tulevaisuuteen, uskalletaan olla aktiivisia ja rohkeita edelläkävijöitä. Strategia ei vaikuta tietoturvallisuuteen liittyvään vastuunjakoon eikä olemassa oleviin organisaatiorakenteisiin. Tämä strategia ja valtiovarainministeriön koordinoima valtionhallinnon tietoturvalinjaukset tukevat toisiaan. Strategialla on linkkejä myös hyväksyttyyn sisäisen turvallisuuden toimintaohjelmaan.

Kansallinen tietoturvastrategia on keskeinen osa hallituksen tietoyhteiskuntapolitiikkaa. Arjen tietoyhteiskunnan neuvottelukunnan toiminta-ohjelmassa 2008–2011 todetaan, että

”Luottamus on tietoyhteiskunnan tärkeimpiä asioita. Luottamus tietoyhteiskuntaan edellyttää teknisesti toimivia ja turvallisia palveluita. Laajasti ymmärrettynä luottamus on käyttäjän kokemus tai näkemys palvelun laadusta. Tavoitteena on luottamuksen ylläpitäminen ja vahvistaminen.

Luottamusta vahvistavat palveluiden helppokäyttöisyys, riittävä kuluttajansuoja, varmuus sisältöjen aitoudesta sekä kuluttajan yksityisyyden ja muiden etujen suojelusta. Kuluttajan aseman parantaminen edellyttää kaikilta toimijoilta vastuullisuutta, myös kuluttajalta itseltään.

Yhteiskunnan toiminnot riippuvat lähes täysin tietoverkkojen ja tietojärjestelmien toimintavarmuudesta. Järjestelmät ovat haavoittuvaisia erilaisille tietoturvauhille ja tietoverkkorikollisuudelle. Toimintaympäristön tietoturvallisuuteen on siten alati kiinnitettävä huomiota, jotta kriittisen infrastruktuurin toiminta ja tietoturvallisuus varmistetaan.”

Strategia luotiin arjen tietoyhteiskunnan neuvottelukunnan alaisessa tietoturvallisuusryhmässä vuoden 2008 aikana lukuisilla työpajoilla, kokouksilla ja haastattelukierroksella. Arjen tietoyhteiskunnan tietoturvallisuusryhmä tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi.

Strategiset tavoitteet

Kansallisen tietoturvastrategian avulla pyritään luomaan suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Yleinen tietoturvaosaamisen pitää olla korkealla tasolla ja yhteiskunnan eri tahot toimivat saumattomassa yhteistyössä tietoturvan edistämiseksi. Suomi on tietoturvan edelläkävijämaa maailmassa vuonna 2015.

Painopiste 1: Perustaidot arjen tietoyhteiskunnassa

Tietoturva on muutakin kuin tekniikkaa. Arjen tietoyhteiskunnassa kansalaiset tarvitsevat uudenlaisia perustaitoja, joita heillä ei aiemmin ollut. Tietoturva nähdään edelleen liiaksi irrallisena osana viestintä- ja tietojärjestelmien kehittämistä. Tietoa on erilaista ja siitä johtuen tulisi miettiä mitä riskejä tiedon turvaamiseen liittyy. Luottamus tietoyhteiskuntaa kohtaan syntyy, kun sekä palveluiden käyttäjät että tuottajat ymmärtävät omat vastuunsa, oikeutensa ja velvollisuutensa. Myös yrittäjien ja yritysten tietoturvasta vastaavien osaamisen kehittäminen on tärkeää.

Painopiste 2. Tietoihin liittyvien riskien hallinta ja toimintavarmuus

Sähköiset palvelut ja asiointi muodostavat yhä keskeisemmän osan niin julkisen kuin yksityisen sektorin palvelujärjestelmää. Samalla riippuvuus tietotekniikasta tekee palveluista entistä haavoittuvaisempia. Kansalaisten on voitava luottaa, että palveluiden käyttö on turvallista ja, että luottamuksellisia tietoja ei joudu vääriin käsiin. Kansalaisille ja yrityksille tulee taata riittävä viranomaistuki, jos tietoturvaa on loukattu esimerkiksi identiteettivarkaustapauksissa.

Painopiste 3: Kilpailukyky ja kansainvälinen verkostoyhteistyö

Suomi elää globaalissa tietoverkkotaloudessa, joten merkittävä osa tietoturvauhista ja –hyökkäyksistä (mm. palvelunestohyökkäykset) kohdistuu meihin maamme rajojen ulkopuolelta. Suomen tulee toimia aktiivisesti kansainvälisessä viranomaisyhteistyössä verkkorikollisuuden ennaltaehkäisemiseksi sekä siitä aiheutuvien haittojen vähentämiseksi. Suomen tulee paitsi kehittää omaa kansallista sääntely-ympäristöään yritysten kannalta yksinkertaisempaan ja ennustettavaan suuntaan myös pyrittävä aktiivisesti vaikuttamaan kansainväliseen sääntelyyn.

Toimenpiteet

1.1. Tietoturvatietoisuuden ja -osaamisen vahvistaminen

Turvallinen toiminta edellyttää perustaitoja niin palveluiden tuottajilta kuin niiden käyttäjiltäkin. Strategialla pyritään varmistamaan, että kansalaisilla on 2000-luvun kansalaistaitoon rinnastettava osaaminen, so. tietoyhteiskunnassa vaadittava tietoturvan lukutaito liittyen verkkopalveluiden käyttöön, omien luottamuksellisten tietojen (salasanat, luottokortti- ja pankkitiedot, henkilötiedot) säilyttämiseen, yleisten verkkohuijausten tunnistamiseen sekä oman päätelaitteen turvallisuudesta huolehtimiseen. Konkreettisia keinoja väestön tietoturvatietoisuuden ja –osaamisen vahvistamiseksi tulisi kehittää.

1.2 Turvallisten sähköisten palveluiden tarjoaminen ja luottamuksellisuuden varmistaminen

Tavoitteena on tehdä kotimaisista verkkopalveluista mahdollisimman turvallisia koko palveluiden elinkaaren aikana (alkaen suunnitteluvaiheesta). Näin tietoturva tulee olennaiseksi osaksi palveluiden laatua. Tämä tarkoittaa käytännössä tietoturvanäkökohtien huomioonottamista myös hankintaprosessien yhteydessä ja palvelusopimuksia tehtäessä. Tietoturvan kehittäminen ei saa olla vain IT-osaajien asia. Johdon rooli on ensi arvoisen tärkeää integroitaessa tietoturva osaksi liiketoiminta- ja hallintoprosesseja. Tietoturvallisuus on huomioitava koko palvelutuotantoketjuun liittyvässä koulutuksessa. Palveluista on tehtävä yksinkertaisia, konkreettisia ja helposti ymmärrettäviä unohtamatta kuitenkaan luottamuksellisten tietojen suojaamista. Yksinkertaisuus tuottaa jo itsessään turvallisuutta.

2.1 Riskienhallinnan ja toimintavarmuuden kehittäminen

Riskien hallinta muodostaa tietoyhteiskunnan tiedon varmistamisen perustan ja takaa järjestelmän toimintavarmuuden ja yritysten liiketoiminnan jatkuvuuden. Riskienhallintanäkökulma tulee aina sisällyttää uusien tuotteiden ja palveluiden suunnitteluun. Yrityksissä riskienhallinta ei ole pelkästään it-asiantuntijoiden tehtävä, vaan se on kyettävä integroimaan kiinteäksi osaksi liiketoiminnan suunnittelua, johtamista ja toteutusta. Yritysten riskienhallintajärjestelmän luominen on johdon asia. Riskien arviointi ja minimointi kuuluu jokaiseen palveluiden kehittämisvaiheeseen. Strategian tehtävänä on edistää riskienhallintamenettelyjen käyttöä. Tämän toiminnan on tapahduttava saumattomassa yhteistyössä viranomaisten, yritysten ja kansalaisten kanssa.

2.2 Yhteiskunnan elintärkeiden toimintojen turvaaminen kaikissa tilanteissa

Yhteiskunnan riippuvuus tieto- ja viestintäjärjestelmistä on hyvin kokonaisvaltaista ja syvenee entisestään. Samalla kuitenkin kilpailu ja pyrkimys kustannustehokkuuteen saattaa vähentää käytettävyyden turvainvestointeja. Arjen tietoyhteiskunnassa yhä suuremmaksi haasteeksi muodostuu entistä monimutkaisempien verkkoja toimintavarmuus ja niiden riskien hallinta. Jo pelkästään internetin kautta tapahtuvaan sähköisten laitteiden ohjaamiseen (esim. katuvalaistuksen ja liikennevalo-ohjauksen siirtyminen internetiin) liittyy suuria riskejä häiriötilanteiden osalta. Yhteisillä harjoituksilla parannetaan varautumista häiriöihin normaalioloissa sekä turvaamaan toiminnan jatkuvuus poikkeusoloissa. Harjoituksissa panostetaan yhteistyömallien luomiseen ja testaukseen. Harjoituksia kehitetään konkreettisen toiminnan suuntaan.

3.1 Suomen houkuttelevuuden ja kilpailukyvyn vahvistaminen ennustettavuutta lisäämällä

Sääntely-ympäristön selkeys ja ennustettavuus on keskeinen tekijä yrityksille. Suomen tulee kehittää lainsäädäntöään siten, että tietoturvakysymyksiin sääntely on mahdollisimman kevyttä ja samalla kattavaa. Viranomaisten tulee lainsäädäntöä kehittäessä kriittisesti tarkastella sen vaikutuksia yritysten toimintaedellytyksiin ja kansalaisten/kuluttajien oikeuksiin (mahdolliset ristiriitanäkökohdat on otettava huomioon). Yhä useampi yritys on monikansallinen ja toimii globaaleilla markkinoilla. Ongelmaksi käytännössä on osoittautunut se, että kansalliset säädökset sekä EU-direktiivien toimeenpano eri maissa eroavat toistaan. Tämä osaltaan vaikeuttaa myös suomalaisten, monessa maassa toimivien, yritysten toimintaedellytyksiä.

3.2 Ennakoivan ja vaikuttavan kansainvälisen yhteistyön terävöittäminen

Ennakoiva ja vaikuttava kansainvälinen toiminta edellyttää hyvää kansallista koordinaatiota ja toimintojen priorisointia. On tärkeää, että kansainvälinen vaikuttaminen aloitetaan riittävän varhaisessa vaiheessa (esim. osallistumalla aktiivisesti valmisteluvaiheen työryhmiin ja epävirallisiin verkostoihin). On tärkeää kartoittaa kansainvälisiä hyviä käytäntöjä sekä kyetä viemään suomalaista tietoturvaosaamista ulkomaille. Lisäksi suomalaisen lainsäädännön ja sääntely-ympäristön edistyksellisyyttä tulee riittävästi ”markkinoida” kansainvälisessä yhteistyössä. Tätä kautta Suomen on mahdollista vaikuttaa muiden maiden

regulaatiokäytäntöihin tavalla, joka palvelee suomalaisten yritysten toimintaa globaaleilla markkinoilla.

Menestyminen kansainvälisen yhteistyössä edellyttää myös aktiivista vaikuttamista EU:n tietoyhteiskuntapolitiikan ja kansainvälisten järjestöjen tietoturvaa koskeviin linjauksiin. Toimivan ja tuloksekkaan NCSA-toiminnon (kansallinen tietoliikenneturvallisuusviranomainen, National Communications Security Authority) perustaminen edistäisi Suomen osallistumista kansainväliseen yhteistyöhön sekä suomalaisten tietotekniikka-alueen toimijoiden osallistumista kansainvälisiin tarjouskilpailuihin. Tietoliikenneturvallisuusviranomaisen rooli kansainvälisen yhteistyön edistäjänä toisi näkyvyyttä suomalaiselle tietoturvaosaamiselle niin viranomais- kuin yritysmaailman kannalta.

Strategian toimeenpano

Lähtökohdat

Nykyisen työjaon mukaan tietoturvallisuus ja tietoturvallisuuden kehittäminen kuuluu voimassa olevan lainsäädännön mukaan usean toimijan vastuulle, sekä yksityisen sektorin että julkisen sektorin vastuulle. Valtioneuvoston ohjesääntöön (262/2003, muutettu 1.1.2008) on kirjattu ministeriöiden työnjako.

Toimeenpanon organisointi

Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Liikenne- ja viestintäministeriön asettaman Arjen tietoyhteiskunnan tietoturvallisuus –ryhmä tukee tämän strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Arjen tietoyhteiskunnan tietoturvallisuus –ryhmässä on laaja-alaisesti toimijoita sekä yksityisen sektorin että julkisen sektorin osalta. Työryhmä antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategiaa sekä raportoi arjen tietoyhteiskunnan neuvottelukunnalle työn etenemisestä.

Arjen tietoyhteiskunnan tietoturvallisuusryhmä perustettiin 31.8.2007 ministeri Suvi Lindénin päätöksellä vuosiksi 1.9.2007 - 28.2.2011. Ryhmän tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi. Ryhmä käsittelee tietoturvaan liittyviä laajoja ja eri sektoreita ylittäviä kysymyksiä läheisessä yhteistyössä muiden tietoturvallisuutta edistävien tahojen kanssa.

Taloudelliset ja yhteiskunnalliset vaikutukset

Periaatepäätöksessä asetetut tavoitteet voidaan toteuttaa kehyspäätösten sekä vuosittain talousarvioin yhteydessä tehtävien päätösten puitteissa. Strategian avulla lisätään kaikkien käyttäjien tietoturvaosaamista ja –tietoisuutta. Strategian avulla lisätään ja vahvistetaan kansallista yhteistyötä tietoturvan osalta.

STATSRÅDETS PRINCIPBESLUT OM EN NATIONELL INFORMATIONSSÄKERHETSSTRATEGI

”Trygg vardag i informationssamhället – Inte med tur utan med kunskap"

Syften med strategin

Med hjälp av den nationella informationssäkerhetsstrategin strävas det efter att skapa finländarna (medborgare, företag, myndigheter och andra aktörer) en trygg vardag i informationssamhället. Strategin har den visionen att medborgarna och företagen kan lita på att deras uppgifter är säkra både på data- och kommunikationsnäten och i tjänsterna som hör till dem. Det allmänna informationssäkerhetskunnandet ska vara på en hög nivå och olika parter i samhället samarbetar friktionsfritt i syfte att främja informationssäkerheten. Finland är föregångarlandet i informationssäkerheten i världen 2015.

Tyngdpunkt 1: Baskunskaper i vardagens informationssamhälle

Tyngdpunkt 2: Riskhantering som anknyter till information och funktionssäkerhet

Tyngdpunkt 3: Konkurrenskraft och internationellt nätverkssamarbete

Åtgärder

Tyngdpunkt 1: Baskunskaper i vardagens informationssamhälle

Varje aktör i informationssamhället verkar genom sina handlingar både i sin egen och i andras informationssäkerhet. Därför är det viktigt att var och en har tillräckliga baskunskaper om informationssäkerheten. Förtroendet för informationssamhället uppstår när både användarna och leverantörerna av tjänster förstår sitt ansvar, sina rättigheter och sina skyldigheter.

Användarna av tjänster måste kunna identifiera och vara medvetna om utgångspunkterna för en säker och pålitlig tjänst. Medborgerliga kunskaper i den elektroniska ärendehanteringen och informationskompetensen är förutsättningar för att man kan röra sig tryggt på webben. Att förutse, identifiera och bereda sig för risker skyddar för många obehagliga överraskningar. Speciellt **tjänsteleverantören** ska säkerställa att det är tryggt att använda tjänsterna och för sin del se till att konfidentiella uppgifter identifieras och skyddas. Tjänsteleverantören har också en skyldighet att se till att tjänstens säkerhet upprätthålls ständigt i och med att omgivningen i tjänsterna och verksamheten ändras.

En öppen och klar kommunikation om tjänstens säkerhet och eventuella risker skapar grunden för det förtroende som behövs för att man kan verka i vardagens informationssamhälle. Tjänsteleverantörens ansvar kan inte läggas ut. I praktiken ska tjänsteleverantören med alla aktörer som deltar i tjänsteproduktionen svara för tjänstens informationssäkerhet. Strategin har till uppgift att integrera

informationssäkerheten till en fast del av informationssamhällets basstrukturer. Detta kräver förutom att den allmänna medvetenheten om och kunnandet i informationssäkerheten stärks också att synpunkterna på informationssäkerheten beaktas då systemen anskaffas och i avtalsprocesserna.

- **Starkare medvetenhet om och kunnande i informationssäkerheten**
    - Projektet för den nationella informationssäkerhetsdagen utvecklas
    - Medvetenheten om informationssäkerheten ökas, dess nivå följs och kunnandet i den utvecklas
    - Det utarbetas en aktiv och förutseende kommunikationsplan

- **Utbud av säkra elektroniska tjänster och säkerställande av förtroendefullheten**
    - Kraven på informationssäkerheten ska bli en del av varje anbudsbegäran, inkl. planeringsfaserna i lösningarna och tjänsterna
    - En vidare användning av lösningarna för informationssäkerheten främjas
    - Möjligheten att utveckla ett separat certifikat som beviljas säkra tjänster utreds
    - En ökning av antalet certifierade sakkunniga som är specialiserade på informationssäkerheten ska främjas i Finland

Tyngdpunkt 2: Riskhantering som anknyter till information och funktionssäkerhet

Elektroniska tjänster och den elektroniska ärendehanteringen bildar en allt centralare del av servicesystemet såväl på den offentliga som på den privata sektorn. Samtidigt gör beroendet av datatekniken tjänsterna sårbarare än tidigare. Medborgarna som använder olika kommunikationstjänster måste kunna lita på att det är tryggt att använda tjänsterna och att konfidentiella uppgifter inte kommer i fel händer. Medborgarna och företagen måste garanteras tillräckligt stöd från myndigheterna om informationssäkerheten har kränkts t.ex. genom identitetsstöld.

När tjänster läggs ut på entreprenad och anskaffningar sammankopplas måste en genomgripande hantering av informationssäkerheten säkerställas. När tjänster planeras ska informationssäkerheten i hela nätet bedömas genomgripande. Leverantören av tjänsten bär här det centrala ansvaret. Förtroendefullheten, integriteten och användbarheten av uppgifterna är väsentliga i servicen.

Funktionen av informationssamhällets kritiska infrastruktur och säkerheten av data- och kommunikationssystemen och kommunikationstjänsterna måste tryggas i alla situationer – från normala förhållanden till undantagsförhållanden. Att företagens verksamhet fortsätter och att medborgarna har tillgång till tjänsterna måste säkerställas.

- **Utveckling av riskhanteringen och funktionssäkerheten**

    - Det ska ges stöd för att den riskhanteringsmodellen som har utvecklats för företagen kan införas i större skala
    - Det ska ordnas utbildning om riskhanteringen

- **Tryggande av samhällets vitala funktioner i alla situationer**

    - Det ska utredas vilka metoder och beredskapsmodeller som ska utvecklas för hanteringen av näten och nätverken som är allt mer invecklade
    - Möjligheten att stöda företagens beredskap och riskhantering utreds
    - Säkerställande av verksamheten av de kommunikationsnät och kommunikationstjänster som samhällets vitala funktioner behöver ska stödas med lagstiftningsåtgärder

Tyngdpunkt 3: Konkurrenskraft och internationellt nätverkssamarbete

Finland ska utveckla sin egen nationella reglering så att den blir enklare och mer förutsebar med tanke på företagen och sträva efter att aktivt påverka den internationella regleringen. Tydligheten av den nationella lagstiftningen och slopande av eventuella hinder för affärsverksamheten påverkar väsentligt den nationella konkurrenskraften och företagens vilja att investera i Finland. Dessutom måste man se till att skillnaderna i den nationella verkställigheten av de EU-direktiv som gäller informationssäkerheten inte oskäligt försvårar verksamheten av de finländska företag som är verksamma i flera EU-länder. Med tanke på ett konkurrenskraftigt informationssamhälle är det nödvändigt att dess centrala kunskapskapital, t.ex. industriella rättigheter och företagshemligheter är skyddade. Genom dessa åtgärder kan man trygga företagens verksamhet i Finland och de finländska företagens verksamhet utomlands och främja det att Finland är ett lockande land för företagen att etablera sig i.

Finland är en del av den globala informationsnätsekonomin och största delen av hoten och angreppen mot informationssäkerheten riktas på oss utanför vårt lands gränser. Bekämpningen av dessa hot kräver en omfattande beredskap och fungerande internationella samarbetsnätverk och ett förutseende handlingssätt och identifiering av svaga signaler. Finland ska agera aktivt i det internationella myndighetssamarbetet för att hoten mot informationssäkerheten kan bekämpas på förhand och att skadorna kan minskas. Globalisationen är inte bara ett hot utan också en möjlighet. För att agera verkningsfullt på internationella forum måste Finland kunna prioritera sin internationella verksamhet och rikta sina resurser på frågor som är viktiga med tanke på informationssäkerheten. För att agerandet är verkningsfullt måste man ha ett bra nationellt samarbete och man ska verka på förhand.

- **Att göra Finland mera lockande och konkurrenskraftigare genom att öka förutsebarheten**

    - Införande av internationella standarder ska främjas och Finland ska aktivt delta i det internationella utvecklingsarbetet av standarderna
    - Finland ska genom EU-samarbetet verka för att direktiven som anknyter till informationssäkerheten verkställs så enhetligt som möjligt. Detta främjar verksamheten hos de finländska företag som är verksamma i flera länder

- **Skärpning av det förutseende och påverkande internationella samarbetet**

    - Inrättande av ett nationellt nätverk för internationellt samarbete ska övervägas. Nätverket ska sprida uppgifter och erfarenheter om de internationella samarbetsgrupperna
    - Det ska utredas behovet av inrättande av en nationell myndighet för informationssäkerheten i Finland (NCSA)

Genomförande av strategin

Statsrådet bär helhetsansvaret för informationssäkerhetsstrategin och övervakar genomförandet av strategin och uppdaterar den efter behov. Gruppen för informationssäkerheten i vardagens informationssamhälle som tillsatts av kommunikationsministeriet stöder samordningen av åtgärderna som genomförandet av strategin kräver samt följer hur strategin verkställs. Gruppen för informationssäkerheten i vardagens informationssamhälle ger statsrådet årligen en berättelse om hur strategin har verkställts och om behovet att uppdatera den samt rapporterar till delegationen för vardagens informationssamhälle om hur arbetet framskrider.

För att målen kan nås utarbetas det utifrån tyngdpunkterna i principbeslutet ett åtgärdsprogram. Åtgärderna, mätarna och uppföljningen som är nödvändiga med tanke på genomförandet av strategin ingår i åtgärdsprogrammet som blir färdigt våren 2009.

MOTIVERINGSPROMEMORIA OM STATSRÅDETS PRINCIPBESLUT OM EN NATIONELL INFORMATIONSSÄKERHETSSTRATEGI

”Trygg vardag i informationssamhället – Inte med tur utan med kunskap”

Bakgrunden för strategin

I den nationella informationssamhällsutvecklingen lever vi nu en fas där data- och kommunikationsteknologin som tidigare var en fristående verksamhetssektor har blivit en del av medborgarnas vardag. I vardagens informationssamhälle (det s.k. ubicompsamhället) blir de datatekniska lösningarna mångsidigare och blir med tanke på användarna en fast del av människornas och företagens normala verksamhet. På grund av detta är det väsentligt att medborgarna kan använda informationssamhällets tjänster enkelt och att de elektroniska tjänsterna upplevs som pålitliga. Alla har ansvar för detta och därför är kunnandet i och medvetenheten om informationssäkerheten väsentligt viktiga. Målet är en trygg vardag i informationssamhället, inte med tur utan med kunskap. Förtroendefullheten, integriteten och användbarheten av uppgifterna har en stor betydelse för vardagens informationssamhälle.

Statsrådets föregående principbeslut om en nationell strategi för informationssäkerheten antogs 2003 och den samlade på ett nästan unikt sätt aktörerna från den privata och den offentliga sektorn runt samma bord. Först och främst lyfte strategin fram informationssäkerheten till ett betydande tema i den samhälleliga debatten. Vår syn på och vårt förstånd om informationssäkerheten har vuxit och Finland har kunnat representera de främsta länderna i ärenden som gäller informationssäkerheten såväl i EU som på internationella forum. Informationssäkerhetsstrategin var den första i Europa och eventuellt den första i världen. Mandattiden för informationssäkerhetsstrategin och den nationella delegationen för informationssäkerhet som samordnade genomförandet av strategin löpte ut våren 2007. Arbetet utfördes mycket betydligt som samarbete mellan den offentliga och den privata sektorn. De största resultaten som informationssäkerhetsstrategin gav var en ökad kunskap om informationssäkerheten bl.a. med införande av en nationell informationssäkerhetsdag, bildande av en nationell lägesbild av informationssäkerheten och resultaten av utvecklingsprogrammet ”Förtroende och informationssäkerhet i elektroniska tjänster”.

Omvärlden förändras snabbt och därför finns det behov att uppdatera informationssäkerhetsstrategin. Det är viktigt att få en realistisk och fokuserad nationell informationssäkerhetsstrategi med några prioriterade mål. Informationssäkerheten ska göras till en väsentlig och naturlig del av det vardagliga livet. Därför skrivs strategin inte bara för sakkunniga inom branschen. Med strategin reagerar vi inte bara passivt utan vi påverkar aktivt framtiden, vågar vara aktiva och modiga föregångare. Strategin påverkar inte ansvarsfördelningen som anknyter till informationssäkerheten och inte heller de existerande organisationsstrukturerna. Strategin och statsförvaltningens riktlinjer för informationssäkerheten som samordnas av finansministeriet stöder varandra. Strategin länkar också till det antagna handlingsprogrammet för den inre säkerheten.

Den nationella informationssäkerhetsstrategin är en central del av regeringens informationssamhällspolitik. I handlingsprogrammet för delegationen för vardagens informationssamhälle för 2008–2011 talas det om informationssäkerheten. Strategin skapades under 2008 i informationssäkerhetsgruppen som lyder under delegationen för vardagens informationssamhälle med hjälp av flera verkstäder, möten och en intervjurunda. Gruppen för informationssäkerheten i vardagens informationssamhälle har till uppgift att främja informationssäkerheten i informationssamhället, följa utvecklingen i fråga om informationssäkerhet och att ta initiativ till att förbättra informationssäkerheten.

Strategiska mål

Med hjälp av den nationella informationssäkerhetsstrategin strävas det efter att skapa finländarna (medborgare, företag, myndigheter och andra aktörer) en trygg vardag i informationssamhället. Strategin har den visionen att medborgarna och företagen kan lita på att deras uppgifter är säkra både på data- och kommunikationsnäten och i tjänsterna som hör till dem. Det allmänna informationssäkerhetskunnandet ska vara på en hög nivå och olika parter i samhället samarbetar skarvlöst i syfte att främja informationssäkerheten. Finland är föregångarlandet i informationssäkerheten i världen 2015.

Tyngdpunkt 1: Baskunskaper i vardagens informationssamhälle

Informationssäkerheten är också annat än teknik. I vardagens informationssamhälle behöver medborgarna nya baskunskaper som de inte tidigare har haft. Informationssäkerheten ses fortfarande för mycket som fristående del från utvecklingen av kommunikations- och datasystemen. Det finns olika slag av information och därför bör man fundera över vilka risker som hör samman med skyddet av information. Förtroendet för informationssamhället uppstår när både användarna och leverantörerna av tjänsterna förstår sitt ansvar, sina rättigheter och sina skyldigheter. Det är också viktigt att utveckla kunnandet hos dem som har hand om företagarnas och företagens informationssäkerhet.

Tyngdpunkt 2: Riskhantering som anknyter till information och funktionssäkerhet

Elektroniska tjänster och den elektroniska ärendehanteringen bildar en allt centralare del av servicesystemet såväl på den offentliga som på den privata sektorn. Samtidigt gör beroendet av datatekniken tjänsterna sårbarare än tidigare. Medborgarna måste kunna lita på att det är tryggt att använda systemen och att konfidentiell information inte kommer i fel händer. Medborgarna och företagen måste garanteras tillräckligt stöd från myndigheterna om informationssäkerheten har kränkts t.ex. genom identitetsstöld.

Tyngdpunkt 3: Konkurrenskraft och internationellt nätverkssamarbete

Finland lever i en global informationsnätsekonomi och således riktas en betydande del av hoten och angreppen (bl.a. överbelastningsattacker) mot informationssäkerheten på oss utanför vårt lands gränser. Finland ska agera aktivt i det internationella

myndighetssamarbetet för att nätbrottsligheten kan bekämpas på förhand och att skadorna som den orsakar kan minskas. Finland ska inte bara utveckla sin egen nationella reglering så att den blir enklare och mer förutsebar med tanke på företagen utan också sträva efter att aktivt påverka den internationella regleringen.

Åtgärder

1.1. Starkare medvetenhet om och kunnande i informationssäkerheten

En trygg verksamhet förutsätter baskunskaper av leverantörerna och användarna av tjänsterna. Med strategin försöker man säkerställa att medborgarna har sådant kunnande som kan likställas med 2000-talets medborgarfärdighet, m.a.o. kunskaper om informationssäkerheten när det handlar sig om användningen av nättjänsterna, förvaring av egna konfidentiella uppgifter (lösenord, kreditkort- och bankuppgifter, personuppgifter), identifieringen av allmänna fall av nätfiske samt översynen av att den egna terminalen är säker. Det bör utvecklas konkreta medel som kan stärka medborgarnas kunskaper och kunnande i informationssäkerheten.

1.2 Utbud av säkra elektroniska tjänster och säkerställande av förtroendefullheten

Målet är att göra de inhemska nättjänsterna så säkra som möjligt under tjänsternas hela livscykel (med början från planeringsfasen). På detta sätt blir informationssäkerheten en väsentlig del av tjänsternas kvalitet. Detta betyder i praktiken att informationssäkerhetsaspekterna beaktas också i samband med anskaffningsprocesserna och när serviceavtal ingås. Utvecklingen av informationssäkerheten får inte vara bara något som hör till IT-sakkunniga. Ledningens roll är ytterst viktig när informationssäkerheten integreras till en del av affärsverksamhets- och förvaltningsprocesser. Informationssäkerheten måste beaktas i utbildningen som hänför sig till hela tjänsteproduktionskedjan. Tjänsterna ska göras så att de är enkla, konkreta och lättförståeliga utan att ändå glömma skyddet av konfidentiella uppgifter. Enkelheten producerar i sig säkerhet.

2.1 Utveckling av riskhanteringen och funktionssäkerheten

Riskhanteringen utgör grunden för säkerställandet av informationssamhällets uppgifter och garanterar systemets funktionssäkerhet och kontinuiteten av företagens affärsverksamhet. Riskhanteringsaspekten ska alltid ingå i planeringen av nya produkter och tjänster. I företagen är riskhanteringen inte bara något som hör till it-sakkunniga utan den ska kunna integreras till en fast del av planeringen, ledningen och genomförandet av affärsverksamheten. Att skapa ett riskhanteringssystem för företagen hör till ledningen. Bedömning och minimering av riskerna hör till varje utvecklingsfas av tjänsterna. Strategin har till uppgift att främja användningen av riskhanteringsförfaranden. Detta ska hända i skarvlöst samarbete med myndigheterna, företagen och medborgarna.

2.2 Tryggande av samhällets vitala funktioner i alla situationer

Samhällets beroende av data- och kommunikationssystemen är mycket genomgripande och blir allt djupare. Samtidigt kan ändå konkurrensen och strävan efter kostnadseffektiviteten minska säkerhetsinvesteringar inom användbarheten. En allt större utmaning i vardagens informationssamhälle blir funktionssäkerheten och riskhanteringen av de allt mer invecklade näten. Till och med styrningen av elektroniska apparater via internet (t.ex. att gatubelysningen och styrningen av trafikljusen överförs till internet) hänger samman med stora risker i störningssituationer. Med gemensamma övningar förbättras i normala förhållanden beredskapen för störningar och strävas efter att fortsätta verksamheten i undantagsförhållanden. Övningarna satsar på att skapa och testa samarbetsmodeller. Övningarna utvecklas så att de innehåller mer konkret verksamhet.

3.1 Att göra Finland mera lockande och att öka konkurrenskraften genom att öka förutsebarheten

Att regelverket är klart och kan förutses är en central faktor för företagen. Finland ska utveckla sin lagstiftning så att regleringen i frågor som gäller informationssäkerheten är så lätt som möjligt och samtidigt täckande. När lagstiftningen utvecklas ska myndigheterna kritiskt betrakta dess verkningar i företagens verksamhetsförutsättningar och medborgarnas/konsumenternas rättigheter (eventuella synpunkter på motstridigheter måste beaktas). Allt flera företag är mångnationella och verkar på globala marknader. Det som i praktiken har visat sig vara problematiskt är att de nationella bestämmelserna och verkställigheten av EU-direktiven i olika länder skiljer sig från varandra. Detta försvårar för sin del verksamhetsförutsättningarna också av de finländska företag som är verksamma i flera länder.

3.2 Skärpning av det förutseende och påverkande internationella samarbetet

En förutseende och påverkande internationell verksamhet behöver en god nationell samordning och prioritering av funktioner. Det är viktigt att det internationella påverkandet inleds i en tillräckligt tidig fas (t.ex. genom aktivt deltagande i beredande arbetsgrupper och inofficiella nätverk). Det är viktigt att kartlägga god internationell praxis och att kunna föra finländskt kunnande i informationssäkerheten till utlandet. Dessutom ska den finländska lagstiftningens och det finländska regelverkets reformvänlighet ”marknadsföras” tillräckligt i det internationella samarbetet. På detta sätt är det för Finland möjligt att påverka andra länders regleringspraxis på ett sätt som gynnar de finländska företagens verksamhet på globala marknader.

Framgång i det internationella samarbetet förutsätter också aktivt påverkande i riktlinjerna för EU:s informationssamhällspolitik och i de internationella organisationernas riktlinjer för informationssäkerheten. Att inrätta en fungerande och resultatrik NCSA-funktion (nationell myndighet för informationssäkerheten, National Communications Security Authority) som främjar Finlands deltagande i det internationella samarbetet och de finländska datateknikaktörernas deltagande i internationella anbudsförfaranden. Rollen som myndigheten för informationssäkerheten har i att främja internationellt samarbete ger synlighet för det finländska informationssäkerhetskunnandet med tanke på myndighets- och företagsvärlden.

Genomförande av strategin

Utgångspunkter

Enligt den nuvarande arbetsfördelningen hör informationssäkerheten och utvecklingen av den enligt den gällande lagstiftningen till flera aktörer; både till den privata sektorn och till den offentliga sektorn. I reglementet för statsrådet (262/2003, ändrat 1.1.2008) har nämnts arbetsfördelningen mellan ministerierna.

Organisering av genomförandet

Statsrådet bär helhetsansvaret för informationssäkerhetsstrategin och övervakar genomförandet av strategin och uppdaterar den efter behov. Gruppen för informationssäkerheten i vardagens informationssamhälle som tillsatts av kommunikationsministeriet stöder samordningen av åtgärderna som genomförandet av strategin kräver samt följer hur strategin verkställs. Gruppen för informationssäkerheten i vardagens informationssamhälle har flera aktörer från den privata sektorn och den offentliga sektorn. Arbetsgruppen ger årligen till statsrådet en berättelse om genomförandet av strategin och behovet att uppdatera den samt rapporterar till delegationen för vardagens informationssamhälle om hur arbetet framskrider.

Gruppen för informationssäkerheten i vardagens informationssamhälle inrättades den 31 augusti 2007 genom beslut av minister Suvi Lindén för tiden 1.9.2007–28.2.2011. Gruppen har till uppgift att främja informationssäkerheten i informationssamhället, följa utvecklingen av informationssäkerheten och att ta initiativ i syfte att förbättra informationssäkerheten. Gruppen behandlar stora frågor som gäller informationssäkerheten och som överskrider olika sektorer i ett nära samarbete med andra parter som främjar informationssäkerheten.

Ekonomiska och samhälleliga verkningar

Målen som ställts i principbeslutet kan förverkligas inom ramen av rambesluten och de beslut som årligen fattas i samband med budgeten. Strategin ökar alla användarnas kunskap i och medvetenhet om informationssäkerheten. Strategin ökar och stärker det nationella samarbetet i fråga om informationssäkerheten.

GOVERNMENT RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

"Everyday security in the information society – a matter of skills, not of luck."

Objectives of the Strategy

The National Information Security Strategy aims to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and for businesses, administrative authorities, and all other actors in society. The Strategy's vision is that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services. There must be a high overall level of information security skills and knowhow, and the different actors in society need to work seamlessly together to improve information security. By 2015 Finland will be the leading country in the world in terms of information security.

Priority 1: Basic skills in the ubiquitous information society

Priority 2: Information risk management and process reliability

Priority 3: Competitiveness and international network cooperation

Measures

Priority 1: Basic skills in the ubiquitous information society

Everyone's actions in the information society have impacts both on their own information security and on that of others. It is therefore important that everyone has adequate basic skills in the field of information security. Trust in the information society is built up when both users and service providers understand their rights and their responsibilities.

Users of electronic services must be able to identify, and be aware of, the underlying principles of secure and reliable service. Internet literacy and a basic national level of skills in using electronic communications are necessary preconditions for the secure use of online services. The ability to anticipate, identify and take precautions against risks can spare the user from many unpleasant surprises. **Service providers** in particular must ensure the security of services and, for their part, also take care that confidential information is identified and protected. The service provider is also responsible for making sure that service security is continuously maintained in the changing service and operational environment.

The provision of clear transparent information about the security of services and the possible risks involved lays the groundwork for the trust that is needed in the ubiquitous information society. The responsibility of the service provider cannot be outsourced. In practice, the service provider is responsible for ensuring that the operations of all players involved in providing the services are secure. The task of the

National Information Security Strategy is to integrate information security firmly into the basic structures of the information society. This requires improvements in general information security awareness and skills, and better consideration of information security aspects in the purchase of systems and the procedures for making agreements.

- **Increasing information security awareness and competence**
    - The National Information Security Day project will be developed.
    - Awareness of information security will be improved, the level of awareness will be monitored and information security skills will be developed.
    - A proactive plan for communications will be drawn up.

- **Providing secure electronic services and ensuring confidentiality**
    - Information security requirements will be incorporated in every invitation to tender, including the planning phases of solutions and services.
    - More extensive use of information security solutions will be promoted.
    - The possibility of introducing special certification for secure services will be investigated.
    - An increase in the number of certified information security professionals in Finland will be promoted.

Priority 2: Information risk management and process reliability

Electronic services and communications are increasingly to be found at the heart of the service system in both the public and the private sectors. At the same time, dependence on information technology is making services more vulnerable than ever. People using the various communication services must be able to trust that the services are secure and that no confidential data will end up in the wrong hands. When a breach of information security occurs, for example in identity theft, people and businesses must be able to rely on adequate support from the authorities.

It is essential to take a holistic approach to information security when services are outsourced and chains of acquisitions are formed. The security of data in the entire network should be evaluated when services are being planned. The primary responsibility for this lies with the service provider. Confidentiality and intactness of data, together with accessibility, are essential elements in the services.

The proper functioning of critical information society infrastructure and the security of ICT systems and services must be ensured at all times, both in normal and emergency conditions. The continuity of business activities and the public's access to services must be fully safeguarded.

- **Improving risk management and service reliability**
    - Support will be provided for the wider adoption of risk management models for businesses.

- Training related to risk management will be arranged.

- **Safeguarding functions that are vital to society in all circumstances**

  - Research will be carried out as to how procedures and response capabilities should be developed for ever more complex networks and network administration.
  - The possibilities of supporting preparedness and risk management in businesses will be explored.
  - Legislative support will be provided to safeguard the communication networks and services necessary for the functions vital to society.

Priority 3: Competitiveness and international network cooperation

Finland should aim to develop a simpler and more predictable national regulation environment for businesses, and actively seek ways to influence the drawing up of international regulations. Clarity of national legislation and the removal of obstacles to business will improve Finnish competitiveness and companies' willingness to invest in Finland. Care must be also taken to make sure that differences in the national implementation of EU directives concerning information security do not unreasonably impede Finnish companies that operate in several Member States. It is crucial for a competitive information society that its most important information and knowledge capital, such as industrial property rights and business secrets, is protected. These measures can safeguard business activities in Finland and the operation of Finnish companies abroad and make Finland more attractive as a corporate location.

Finland is part of the global information network economy, and most information security threats and attacks come from outside the country's borders. Prevention of these threats requires not only comprehensive preparedness and efficient networks of international cooperation but also a forward-looking approach and the identification of signs and signals of threats, however weak. Finland must be active in international cooperation between national authorities to prevent information security threats and minimise any possible damage. Globalisation is not just a threat but also an opportunity. To act effectively in international forums, Finland must be able to prioritise its international activities and allocate resources to key information security issues. Effectiveness can only be achieved through good national cooperation and exerting an influence on decisions before they are made.

- **Increasing Finland's attractiveness and competitiveness through better predictability**

  - Promotion of the adoption of international standards and active participation in international development work.
  - Active involvement in EU cooperation to ensure that information security directives are implemented in as uniform a way as possible and so also promote the activities of Finnish companies operating in several countries.

- **Intensifying forward-looking and influential international cooperation**
    - The creation of a national network for the purpose of exchanging information and experiences of international working groups will be considered.
    - The need to establish a National Communications Security Authority (NCSA) in Finland will be examined.

Implementation of the Strategy

The overall responsibility for the National Information Security Strategy lies with the Government, which supervises the Strategy's implementation and updates it when necessary. The Information Security Group of the Ubiquitous Information Society Advisory Board appointed by the Ministry of Transport and Communications supports the coordination of the Strategy's implementation and monitors the implementation process. The Information Security Group submits an annual report to the Government on the implementation of the Strategy and on the need to update it, and reports to the Ubiquitous Information Society Advisory Board on the progress of the work.

In order to attain the Strategy's goals, an action plan will be drawn up based on the priorities set out in this Resolution. The measures, indicators, monitoring and follow-up necessary for the implementation of the Strategy will be included in the action plan, which will be completed by spring 2009.

EXPLANATORY MEMORANDUM CONCERNING THE GOVERNMENT RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

"Everyday security in the information society – a matter of skills, not of luck"

Background to the Strategy

In Finland today, the information society has reached the stage at which information and communications technologies are no longer separate sectors of society but have become part of people's everyday lives. In the ubiquitous information society the diversity of IT solutions is increasing and these solutions are becoming an integral part of people's daily activities and normal business operations. It is therefore important that everyone has easy access to information society services, and that the electronic services are felt to be reliable. This is a collective responsibility, so people's awareness of information security and their competence in dealing with it are particularly important. The aim of everyday security in the information society will be achieved through everybody's skills and good judgment, not just by luck. The confidentiality, integrity and accessibility of data are very important elements of today's information society.

The previous government resolution on national information security strategy was adopted in 2003 and it brought actors in both the private and the public sectors together in an almost unprecedented way. Above all, it drew attention to and encouraged discussion about information security. Awareness and competence in information security have grown and Finland has been one of the leading countries in the field, both within the EU and internationally. The strategy was the first of its kind in Europe and possibly in the world. The term of office for the National Information Security Advisory Board that coordinated the implementation of the strategy expired in spring 2007. The most significant results of the information security strategy of 2003 included an increase in information security awareness (for example by establishing a national Information Security Day), the compiling of a review of the national information security situation, and the results of a development programme entitled "Trust and information security in electronic services".

The operational environment changes quickly, so information security strategy has to be updated. It is important that the national strategy is realistic and focused, and that it includes prioritised objectives. Information security must be made an integral and natural part of everyday life. The National Information Security Strategy is not addressed to experts only. It is not just a strategy of passive reaction but of actively influencing the future and encouraging bold pioneering. The Strategy does not affect the existing division of responsibilities for information security or the existing organisational structures. The Strategy set out in the government resolution and the State Information Security Guidelines coordinated by the Ministry of Finance complement one another. The Strategy is also linked to the Internal Security Programme.

The National Information Security Strategy is an essential element of the Government's information society policy. The Action Programme 2008-2011 of the Ubiquitous Information Society Advisory Board states that

> *"Trust is one of the most important information society issues. Trust in the information society requires technically efficient and secure services. Trust, broadly understood, is the user's experience or view of service quality. The goal is to maintain and strengthen this trust.*
>
> *Trust is strengthened by easy-to-use services, adequate consumer protection, and confidence in content authenticity as well as protection of consumer privacy and other interests. Improving the position of consumers requires responsibility to be exercised by all parties, including consumers themselves.*
>
> *Society's functions depend almost entirely on the reliability of information networks and systems. Systems are vulnerable to various information security threats and internet crime. Operating environment information security must therefore always be taken into consideration in order to safeguard the operation of critical infrastructure and ensure the integrity of data."*

The Strategy was drawn up in 2008, with the aid of numerous workshops, conferences and rounds of interviews, by the Information Security Group that works under the Ubiquitous Information Society Advisory Board. The tasks of the Information Security Group are to promote information security in the information society, monitor the progress that is made, and suggest improvements.

Strategic aims

The National Information Security Strategy aims to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and for businesses, administrative authorities, and all other actors in society. The Strategy's vision is that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services. There must be a high overall level of information security skills and knowhow, and the different actors in society need to work seamlessly together to improve information security. By 2015 Finland will be the leading country in the world in terms of information security.

Priority 1: Basic skills in the ubiquitous information society

Information security involves more than just technology. In the ubiquitous information society, people need new kinds of basic skills that they did not possess before. Information security is still too often seen as being a disconnected part of overall ICT development. There are many kinds of information, and information security risks should be evaluated on the basis of the type of data concerned. Trust in the information society is built upon the service providers' and users' understanding of their rights and responsibilities. It is also important to improve the skills of business owners and corporate information security professionals.

Priority 2: Information risk management and process reliability

Electronic services and communications are increasingly to be found at the heart of the service system in both the public and private sectors. At the same time, dependence on information technology is making services more vulnerable. People must be able to trust that the services they use are secure and that no confidential data will end up in the wrong hands. When a breach of information security occurs, for example in identity theft, people and businesses must be able to rely on adequate support from the authorities.

Priority 3: Competitiveness and international network cooperation

Finland is part of the global information network economy, which means that a significant percentage of information security threats and attacks (e.g. denial-of-service attacks) originate outside the country's borders. Finland must be active in international cooperation between national authorities to prevent information security threats and minimise any possible damage. As well as making its own national regulatory environment simpler and more predictable for businesses, Finland must actively seek ways of influencing international regulation.

Measures

1.1. Increasing information security awareness and competence

Secure operations call for basic skills from both the providers and users of the services. The Strategy aims to ensure that everyone in Finland possesses a basic general competence in the 21st century skills needed in the information society, particularly the "information security literacy" related to use of network services, storage of confidential data (passwords, credit card and bank account details, personal data), recognition of common cases of phishing, and ways of ensuring the security of one's own data terminal equipment. Concrete ways of improving people's information security awareness and skills must be explored and developed.

1.2 Providing secure electronic services and ensuring confidentiality

The aim is to make Finnish network services as secure as possible throughout their entire life span, starting right from the beginning at the design and planning stage. In this way, information security will become an integral part of service quality. This

means in practice that information security aspects are also to be taken into consideration in the processes for purchasing systems and making service agreements. Information security development cannot be left to IT experts alone: the role of senior management is of prime importance in the integration of information security into business and administrative processes. Attention must also be paid to information security in each phase of training throughout the service provision chain. Services must be made simple, concrete and easy to understand, but without forgetting safeguards for confidential information. Simplicity also promotes security.

2.1 Improving risk management and service reliability

Risk management is the cornerstone of data security in the information society. It ensures the reliability of systems and the continuity of business operations. Risk management perspectives must always be taken into account in designing new products and services. In businesses, risk management is not just the IT experts' responsibility but must be firmly integrated into business planning, management and operations. The creation of a risk management system for a company is a responsibility of that company's senior management. Each stage of service development should include risk evaluation and minimization. One of this Strategy's main tasks is to promote the use of risk management procedures. This must be carried out in seamless cooperation between the authorities, businesses and citizens.

2.2 Safeguarding functions that are vital to society in all circumstances

Today's society is highly dependent on ICT systems and this dependence is steadily increasing. At the same time, however, competition and efforts to improve cost-efficiency may result in a decrease of investment in security. In the ubiquitous information society, the reliability of increasingly complex networks and the management of possible risks pose ever greater challenges. The control of electronic equipment and systems through the Internet (for example online control of traffic lights and street lighting) is just one area that involves serious risks in terms of service disruptions. Joint training exercises improve preparedness for disruptions under normal conditions, and ensure the continuity of service even in emergency conditions. The training emphasises the creation and testing of optimal ways of joint cooperation. The training is also being increasingly oriented towards concrete activities.

3.1 Increasing Finland's attractiveness and competitiveness through better predictability

The clarity and predictability of the regulatory environment is of great importance to companies. Finland should develop its legislation so that the regulatory framework for information security is as light as possible and at the same time comprehensive in scope. The administrative authorities must critically observe the impacts of legislation on the operating conditions for businesses and on people's rights as citizens and as consumers, paying particular attention to any aspects that may be contradictory. More and more businesses are multinational organisations that operate in the global market. In practice, the fact that different countries have different national regulations and implement EU directives in different ways has proved to be a problem. It also complicates the operating conditions for Finnish companies that are active in several countries.

3.2 Intensifying forward-looking and influential international cooperation

Forward-looking and influential international cooperation calls for good national coordination and prioritisation. It is important that influence starts to be exerted in the international arena at a sufficiently early stage (for example through active participation in preparatory working groups and unofficial networks). It is also important to identify good international practices and to be able to export Finnish information security knowhow to other countries. The progressive nature of Finland's legislation and regulatory environment must be adequately "marketed" in forums of international cooperation. By doing this, Finland can also influence the regulatory practices of other countries in a way that benefits Finnish businesses operating in the global market.

Success in international cooperation also depends on playing an active part in developing guidelines for EU information society policy and for the information security policy of international organisations. The establishment of an efficient and effective National Communications Security Authority (NCSA) would promote Finland's participation in international cooperation as well as Finnish IT operators' participation in international tendering procedures. The role of the NCSA in promoting international cooperation would give Finnish information security skills and knowhow better visibility in the eyes of governmental organisations and the business world.

Implementation of the Strategy

Starting points

Under the current legislation and division of responsibilities, information security and its development are the responsibility of a number of parties, and a responsibility of both the private and public sectors. The responsibilities of each Ministry are set out in the Government Rules of Procedure (262/2003, amended 1 January 2008).

Arrangements for implementation

The overall responsibility for the National Information Security Strategy lies with the Government, which monitors the Strategy's implementation and updates it when necessary. The Information Security Group of the Ubiquitous Information Society Advisory Board appointed by the Ministry of Transport and Communications supports the coordination of the measures required to implement the Strategy and monitors its implementation. The Information Security Group includes representatives of both private and public sectors on a broad basis. The working group reports annually to the Government on the implementation of the Strategy and on needs for updating it. It also reports to the Ubiquitous Information Society Advisory Board on the progress of the work being done.

The Information Security Group of the Ubiquitous Information Society Advisory Board was appointed on 31 August 2007 by Ms Suvi Lindén, Minister of

Communications, for the period from 1 September 2007 to 28 February 2011. The Group's task is to promote, monitor and suggest improvements for information security in the information society. The group deals with broad, cross-sectoral issues about information security and works in close cooperation with other parties and organisations that promote information security.

Economic and social impacts

The aims set out in the Resolution can be achieved within the framework of decisions on spending limits and the annual Budget. The Strategy will help to increase information security awareness and competence among all users, and to increase and strengthen national cooperation in the whole field of information security.

ASETTAMISPÄÄTÖS LVM 073:01/2007
31.8.2007

Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä

Asettaminen

Liikenne- ja viestintäministeriö on asettanut arjen tietoyhteiskunnan neuvottelukunnan alaisen arjen tietoyhteiskunnan tietoturvallisuus -ryhmän.

Toimikausi

1.9.2007 - 28.2.2011

Tausta

Valtioneuvosto hyväksyi 21.6.2007 periaatepäätöksen tietoyhteiskuntapolitiikasta ja asetti samalla arjen tietoyhteiskuntaneuvottelukunnan varmistamaan kansallisen tietoyhteiskuntastrategian käytännön toteutuksen. Periaatepäätöksen mukaisesti neuvottelukunnan yhteyteen asetetaan tietoturvallisuuden asiantuntijaryhmä.

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi hyväksyttiin syyskuussa 2003. Tietoturvastrategian ja siihen kuuluvan kansallisen tietoturvallisuusasioiden neuvottelukunnan toimikausi loppui keväällä 2007. Uusi arjen tietoyhteiskunnan tietoturvallisuusryhmä on jatkoa tälle työlle.

Tehtävä

Arjen tietoyhteiskunnan tietoturvallisuus -ryhmän tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi. Ryhmä käsittelee tietoturvaan liittyviä laajoja ja eri sektoreita ylittäviä kysymyksiä. Tämän lisäksi ryhmä vastaa uuden tietoturvastrategian luomisesta sekä sen yhteiskunnallisesti keskeisimmän toimeenpanon koordinoimisesta. Ryhmä toimii läheisessä yhteistyössä muiden tietoturvallisuutta edistävien tahojen kanssa.

Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä tulee kiinnittämään huomiota sekä tämän päivän että tulevaisuuden haasteisiin tietoturvaan liittyen. Työryhmä tulee toimimaan kansallisena ”think-tank”:inä tietoturvakysymyksissä. Ryhmä tulee rohkeasti nostaa esille myös kiistanalaisia tietoturvaan liittyviä kysymyksiä sekä toimia vahvasti keskustelevana.

Toimikunnan kokoonpano

Puheenjohtaja

Juhapekka Ristola	yksikön päällikkö, viestintäneuvos	Liikenne- ja viestintäministeriö

Jäsenet

Aarnio, Reijo	tietosuojavaltuutettu	Tietosuojavaltuutetun toimisto
Bergius, Kimmo	turvallisuusjohtaja	Microsoft
Candolin, Catharina	tietohallintopäällikkö	Puolustusvoimat
Heliö, Erkki	turvallisuusjohtaja	Tietoenator
Hyppönen, Mikko	tutkimusjohtaja	F-Secure
Härkönen, Juha	turvallisuusjohtaja	Fortum
Järvinen, Kari	johtaja	Elisa
Järvinen, Petteri	tutkija	Petteri Järvinen Oy
Kiviniemi, Mikael	neuvotteleva virkamies	Valtiovarainministeriö
Kylänlahti, Henry	yritysturvallisuusjohtaja	TeliaSonera Finland Oyj
Lappi, Jaana	ylitarkastaja	Kauppa- ja teollisuusministeriö
Lauhde, Mika	johtaja	Nokia
Lehtimäki, Timo	johtaja	Viestintävirasto
Loikala, Veli-Pekka	rikosylikomisario	Keskusrikospoliisi
Nieminen, Pete	palvelutuotepäällikkö	IBM Finland
Oksanen, Kari	riskienhallintajohtaja	Nordea
Särs, Jonna	johtava konsultti	Nixu
Wirman, Kari	varautumispäällikkö	FiCom ry

Sihteeri

Mari Herranen	neuvotteleva virkamies	Liikenne- ja viestintäministeriö

Työryhmän jäsenet on valittu tehtävään asemansa perusteella, mistä syystä ei ole voitu ottaa huomioon tasa-arvolain 4 §:n 2 momentin vaatimuksia.

Toimijat vastaavat kukin omista kustannuksistaan.

Viestintäministeri

Suvi Lindén

Kansliapäällikkö

Harri Pursiainen

JAKELU Työryhmän jäsenet ja sihteeri
LVM:n kirjaamo

APPOINTMENT DECISION LVM 073:01/2007
31 August 2007

Information security group of the Ubiquitous Information Society Advisory Board

Appointment

The Ministry of Transport and Communications has appointed an information security group under the Ubiquitous Information Society Advisory Board.

Term of office

1 September 2007 – 28 February 2011

Background

The Finnish Government adopted a resolution on information society policy on 21 June 2007 and appointed a Ubiquitous Information Society Advisory Board for ensuring the practical implementation of the information society strategy. In accordance with the resolution an expert group on information security is to be appointed in connection with the Advisory Board.

A Government resolution on the national information security strategy was adopted in September 2003. The term of office of the National Information Security Advisory Board, and the information security strategy, expired in the spring 2007. The work will continue in this new information security group of the Ubiquitous Information Society Advisory Board.

Mission

The tasks of the information security group will be to promote, monitor and suggest improvements in information security. The group will discuss broad, cross-sectoral issues about information security, and it will be responsible for outlining a new information security strategy and for coordinating the implementation of the strategy's most important elements in society. It will work in close cooperation with other parties involved in information security promotion.

The group will pay attention to present and future challenges in information security, and act as a national "think-tank" in information security issues. The group should also firmly and determinedly draw attention to controversial issues in information security, too, and encourage discussion.

Group members

Chair

Juhapekka Ristola	Director of Media and Communications Services Unit	Ministry of Transport and Communications

Members

Aarnio, Reijo	Data Protection Ombudsman	Office of the Data Protection Ombudsman
Bergius, Kimmo	Chief Security Advisor	Microsoft
Candolin, Catharina	Chief of Information Management	Finnish Defence Forces
Heliö, Erkki	Chief Security Officer	Tietoenator
Hyppönen, Mikko	Chief Research Officer	F-Secure
Härkönen, Juha	Head of Corporate Security	Fortum
Järvinen, Kari	Director	Elisa
Järvinen, Petteri	Researcher	Petteri Järvinen Oy
Kiviniemi, Mikael	Chief Counsellor	Ministry of Finance
Kylänlahti, Henry	Director	TeliaSonera Finland Oyj
Lappi, Jaana	Senior Adviser	Ministry of Trade and Industry
Lauhde, Mika	Director	Nokia
Lehtimäki, Timo	Director	Finnish Communications Regulatory Authority
Loikala, Veli-Pekka	Detective Superintendent	National Bureau of Investigation
Nieminen, Pete	Service Product Line Leader	IBM Finland
Oksanen, Kari	Director	Nordea
Särs, Jonna	VP, Head of Information Security	Nixu
Wirman, Kari	Manager of Telecommunications Preparedness	FiCom ry

Secretary

Mari Herranen	Ministerial Adviser	Ministry of Transport and Communications

The members have been appointed to the group on the basis of their organisational position, and, therefore, section 4(2) of the Gender Equality Act could not be considered in the appointment process.

The members will themselves be responsible for the expenses incurred in the work.

Minister of Communications

Suvi Lindén

Permanent Secretary Harri Pursiainen

DISTRIBUTION Members and secretary of the working group
Registration of the Ministry of Transport and Communications

Arjen tietoyhteiskunnan neuvottelukunnan alainen tietoturvallisuusryhmä / Gruppen för informationssäkerheten i vardagens informationssamhälle / Information Security Group of the Ubiquitous Information Society Advisory Board

1.1.2009 / 1 January 2009

Mari Herranen (pj./ordf./chair)
neuvotteleva virkamies / Ministerial Adviser
liikenne- ja viestintäministeriö / Ministry of Transport and Communications

Timo Kievari (siht./sekr./secretary)
ylitarkastaja / Senior Officer
liikenne- ja viestintäministeriö / Ministry of Transport and Communications

Reijo Aarnio
tietosuojavaltuutettu / Data Protection Ombudsman
Tietosuojavaltuutetun toimisto / Office of the Data Protection Ombudsman

Kimmo Bergius
turvallisuusjohtaja / Chief Security Advisor
Microsoft Oy

Catharina Candolin
tietohallintopäällikkö / Chief of Information Management
Puolustusvoimat / Finnish Defence Forces

Olli Haukkovaara
tietoturvapäällikkö / Information Security Manager
TeliaSonera Finland Oyj

Erkki Heliö
turvallisuusjohtaja / Chief Security Officer
TietoEnator

Mikko Hyppönen
tutkimusjohtaja / Chief Research Officer
F-Secure

Juha Härkonen
turvallisuusjohtaja / Head of Corporate Security
Fortum

Antti Järvinen
tietoturvapäällikkö / Information Security Manager
Kesko Oyj

Petteri Järvinen
tutkija / Researcher
Petteri Järvinen Oy

Satu Kiiskinen
tarjoomajohtaja / Vice President, Corporate Customer Solutions
Elisa Oyj

Mikael Kiviniemi
neuvotteleva virkamies / Chief Counsellor
valtiovarainministeriö / Ministry of Finance

Veli-Pekka Kuparinen
johtaja / Managing Director
Huoltovarmuuskeskus / National Emergency Supply Agency

Henry Kylänlahti
johtaja / Fraud and Dispute Manager
Luottokunta

Jaana Lappi
ylitarkastaja / Senior Adviser
työ- ja elinkeinoministeriö / Ministry of Employment and Economy

Mika Lauhde
Director
Nokia, Technology Management, Customer and Market Operations

Timo Lehtimäki
johtaja / Director
Viestintävirasto / Finnish Communications Regulatory Authority

Veli-Pekka Loikala
rikosylikomisario / Detective Superintendent
Keskusrikospoliisi / National Bureau of Investigation

Kari Oksanen
riskienhallintajohtaja / Director
Nordea

Jonna Särs
johtaja konsultti / VP, Head of Information Security
Nixu

Kalevi Tiihonen
yritysturvallisuustoimiston päällikkö / Head of Bureau Corporate Security
Elinkeinoelämän keskusliitto / Confederation of Finnish Industries

Kari Wirman
varautumispäällikkö / Manager of Telecommunications Preparedness
FiCom ry